EUROPEAN PATENT OFFICE

Patent Abstracts of Japan

PUBLICATION NUMBER : 11039219
PUBLICATION DATE : 12-02-99

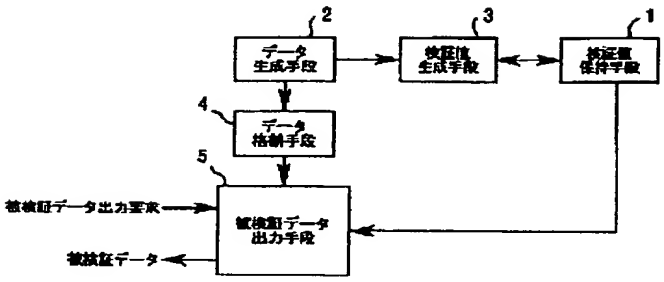
APPLICATION DATE : 18-07-97
APPLICATION NUMBER : 09193535

APPLICANT : FUJI XEROX CO LTD;

INVENTOR : SAITO KAZUO;

INT.CL. : G06F 12/14 G06F 9/06 G09C 1/00 G09C 1/00 H04L 9/32

TITLE : DATA-TO-BE-VERIFIED GENERATING DEVICE, DATA VERIFYING DEVICE, AND MEDIUM RECORDING VERIFIED DATA GENERATING PROGRAM



ABSTRACT : PROBLEM TO BE SOLVED: To generate data which can be kept in a terminal device in such a state that the data is not used in an unauthorized state and for which the compatibility of order is guaranteed.

SOLUTION: A verified value holding means 1 holds a verified value and a data generating means 2 generates a data main body at prescribed timing. A verified value generating means 3 generates a new verified value based on the verified value held by the holding means 1 and a newly generated data main body whenever the data generating means 2 generates a data body and updates the verified value held by the holding means 1 with the new verified value. A data storing means 4 successively stores the data bodies generated by means of the data generating means 2. A data-to-be-verified outputting means 5 generates an authenticator based on the verified value held by the holding means 1 and outputs data to be verified which are generated by coupling the generated authenticator with the data main body stored in the data storing means 4 upon receiving a data-to-be-verified outputting request.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－39219

(43)公開日　平成11年(1999)２月12日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	12/14	３１０	Ｇ０６Ｆ	12/14	３１０Ｚ
	9/06	５５０		9/06	５５０Ｚ
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ａ
		６６０			６６０Ａ
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７３Ｅ

審査請求　未請求　請求項の数９　ＯＬ　（全 15 頁）

(21)出願番号　特願平9－193535

(22)出願日　平成９年(1997)７月18日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72)発明者　河野　健二
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

(72)発明者　田口　正弘
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

(72)発明者　齊藤　和雄
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

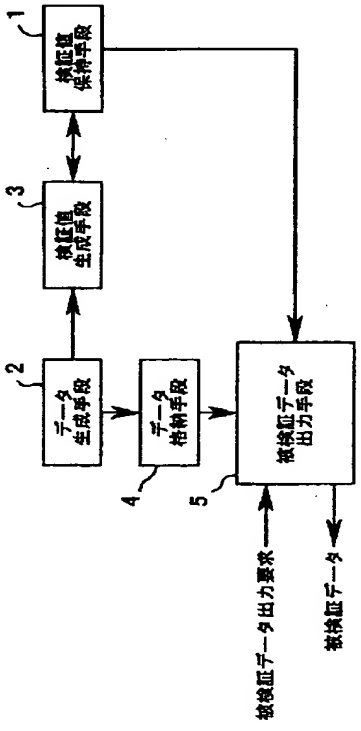
(74)代理人　弁理士　服部　毅巖

(54)【発明の名称】　被検証データ生成装置、データ検証装置及び被検証データ生成プログラムを記録した媒体

(57)【要約】

【課題】　不正操作を受けること無く端末装置に保管可能であり、且つ順番の整合性が保証されたデータを生成できるようにする。

【解決手段】　検証値保持手段１は、検証値を保持する。データ生成手段２は、所定のタイミングでデータ本体を生成する。検証値生成手段３は、データ生成手段２によりデータ本体が生成される度に、検証値保持手段１において保持されている検証値と新たに生成されたデータ本体とに基づいて新たな検証値を生成する。そして、新たな検証値で検証値保持手段１に保持されている検証値を更新する。データ格納手段４は、データ生成手段２で生成されたデータ本体を順次格納する。被検証データ出力手段５は、被検証データ出力要求を受け取ると、検証値保持手段１に格納されている検証値に基づいて認証子を生成し、生成した認証子とデータ格納手段４に格納されているデータ本体とを結合した被検証データを出力する。



【特許請求の範囲】
【請求項１】　被検証データを生成する被検証データ生成装置において、
検証値を保持する検証値保持手段と、
データ本体を生成するデータ生成手段と、
前記データ生成手段によりデータ本体が生成される度に、前記検証値保持手段において保持されている検証値と新たに生成されたデータ本体とに基づいて新たな検証値を生成し、生成した検証値で前記検証値保持手段に保持されている検証値を更新する検証値生成手段と、
前記データ生成手段で生成されたデータ本体を順次格納するデータ格納手段と、
被検証データ出力要求を受け取ると、前記検証値保持手段に格納されている検証値を用いて署名値を生成し、前記データ格納手段に格納されているデータ本体と前記署名値とを含む被検証データを出力する被検証データ出力手段と、
を有することを特徴とする被検証データ生成装置。
【請求項２】　データ消去要求に応じて、前記データ格納手段に格納されているデータ本体を消去するデータ消去手段と、
前記データ消去手段によって前記データ格納手段内のデータが消去される度に設定されている値をカウントする被検証データシリアル番号カウンタとをさらに有し、
前記被検証データ出力手段は、被検証データ出力要求を受け取った際の前記被検証データシリアル番号カウンタの値を前記被検証データに含めて出力することを特徴とする請求項１記載の被検証データ生成装置。
【請求項３】　前記検証値生成手段は、一方向性関数を用いて新たな検証値を生成することを特徴とする請求項１記載の被検証データ生成装置。
【請求項４】　前記データ生成手段によるデータ本体の生成条件を保持するデータ生成条件保持手段と、
前記データ生成条件が満たされなくなった時点で、所定のデータ処理機能を停止する機能停止手段と、
利用延長データを受け取ると、前記利用延長データを認証する利用延長データ認証手段と、
前記利用延長データ認証手段が認証に成功した場合に、前記データ処理機能の機能停止を解除する機能停止解除手段と、
をさらに有することを特徴とする請求項１記載の被検証データ生成装置。
【請求項５】　前記利用延長データ認証手段は、受け取った利用延長データから照合用検証値を抽出し、前記照合用検証値と前記検証値保持手段に保持されている検証値とが一致した場合に限り前記利用延長データを認証することを特徴とする請求項４記載の被検証データ生成装置。
【請求項６】　前記利用延長データ認証手段は、受け取った前記利用延長データから照合用検証値を抽出するとともに、前記データ格納手段内のデータ本文を格納された順に選択し、最初に選択されたデータ本文と前記照合用認証値とから前記検証値生成手段と同じ方法で新たな検証値を生成し、以後、選択されたデータ本文と直前に生成された検証値とから新たな検証値を順次生成し、最後に生成された検証値と前記検証値保持手段に保持されている検証値とが一致した場合に限り前記利用延長データを認証することを特徴とする請求項４記載の被検証データ生成装置。
【請求項７】　前記被検証データ出力手段が被検証データを出力した時点で前記検証値保持手段に保持されている検証値をデータ出力時検証値として保持するデータ出力時検証値保持手段を更に有し、
前記利用延長データ認証手段は、受け取った前記利用延長データから照合用検証値を抽出し、前記照合用検証値と前記データ出力時検証値保持手段に保持されているデータ出力時検証値とが一致している場合に限り前記利用延長データを認証することを特徴とする請求項４記載の被検証データ生成装置。
【請求項８】　データの検証を行うデータ検証装置において、
検証値を保持する検証値保持手段と、
複数のデータ本文に対して署名値が付加された被検証データを受け取ると、前記検証値保持手段に保持されている検証値と前記複数のデータ本文とから照合用検証値を生成する照合用検証値生成手段と、
前記署名値から求められる検証値と前記照合用検証値とを照合し、一致した場合にのみ前記被検証データの内容が正しいと認める認証手段と、
前記署名値から求められる検証値と前記照合用検証値とが一致した場合には、前記照合用検証値によって前記検証値保持手段に保持されている検証値を更新する検証値更新手段と、
を有することを特徴とするデータ検証装置。
【請求項９】　被検証データの生成をコンピュータに行わせるための被検証データ生成プログラムを記録した媒体において、
検証値を保持する検証値保持手段、
データ本体を生成するデータ生成手段、
前記データ生成手段によりデータ本体が生成される度に、前記検証値保持手段において保持されている検証値と新たに生成されたデータ本体とに基づいて新たな検証値を生成し、生成した検証値で前記検証値保持手段に保持されている検証値を更新する検証値生成手段、
前記データ生成手段で生成されたデータ本体を順次格納するデータ格納手段、
被検証データ出力要求を受け取ると、前記検証値保持手段に格納されている検証値を用いて署名値を生成し、前記データ格納手段に格納されているデータ本体と前記署名値とを含む被検証データを出力する被検証データ出力

手段、
としてコンピュータを機能させるための被検証データ生成プログラムを記録した媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は被検証データ生成装置、データ検証装置及び被検証データ生成プログラムを記録した媒体に関し、特にデータ群に署名を施して被検証データを生成する被検証データ生成装置、署名が施された被検証データを検証するデータ検証装置及びデータ群に署名を施すための被検証データ生成プログラムを記録した媒体に関する。
【０００２】
【従来の技術】近年のネットワークの発達によって、さまざまな情報がディジタル化されネットワークを通じて流通する時代が到来している。ディジタル化される情報としては、文字情報をはじめ静止画、動画、音声、プログラムなどがあり、我々はネットワーク上でこれらを組み合わせたさまざまなサービスを受けることが可能である。しかし、これらディジタル情報の大きな特徴であるコピーの容易性が、これまでネットワークでのディジタル情報の流通を阻害する要因となっていた。これは、ディジタル情報をコピーするとオリジナルとまったく同じ物を生成することができるため、一旦流通したものが著作者の意図しないところで無断で使用され、著作者が得るべき正当な対価を回収し難いという問題に起因する。
【０００３】この問題を解決するため、最近ではＣＤ－Ｓｈｏｗｃａｓｅ（米International Business Machines 社の登録商標）のように、ディジタル情報を暗号化して自由に流通させ、利用する際には代金を支払って電話回線等で復号鍵を受け取り、ディジタル情報を利用するようなシステムも登場している。ただし、この方法では、利用頻度に応じて課金することが出来ない。
【０００４】利用頻度に応じて課金するには、利用履歴等の課金情報を回収する必要がある。そして、利用履歴を回収するに当たっては、利用履歴もまたディジタル情報であるためその正当性を保証する仕組みが必要となる。
【０００５】そこで、特開平３－２５６０５号公報の「課金情報送出方式」および特開平６－１８０７６２号公報の「課金情報収集システム」に開示されているように、課金情報を出力する装置を通信回線で結んで自動的に課金情報を回収することが考えられている。なお、通信回線を利用する場合は、ＲＳＡ(Rivest, Shamir, Adleman) 暗号を利用した電子署名方式（岡本栄司著：暗号理論入門、共立出版、ｐｐ．１３４－１３８（１９９３））等により、課金情報の正当性を保証できる。
【０００６】なお、上記の例は、ディジタル情報を利用する端末が常にネットワークにつながっていることが前提となっている。それは、オフラインの端末装置に履歴データを長期にわたって蓄積すると、ユーザの恣意的な管理や、システムの事故などの危険にさらされるという弊害があるためである。ところが、一般的なユーザはディジタル情報をオフラインで利用することがほとんどである。そのため、ユーザの端末を常にネットワークで管理することは通信コストやシステムの運用性を考えると受け入れ難いものであるといえる。
【０００７】一方、秘密情報を保持する媒体としてＩＣ(Integrated Circuit)カードが注目を集めている。このＩＣカードを用いれば、課金情報等を安全に回収することができる。ＩＣカードを用いて課金情報を回収するものとして、例えば、特公平６－９５３０２号公報の「ソフトウエア管理方式」がある。これには、ソフトウエアを利用した量に応じて課金し、料金を回収するシステムの例が示されている。この例によれば、ユーザは所定の代理店でＩＣカードを購入し、購入した代金に応じた金額がＩＣカードの残高メモリに書き込まれる。ユーザがソフトウエアを起動する際にＩＣカード内の残高メモリをチェックし、そのソフトウエアの利用価格分の金額を残高メモリから減算する。ユーザは、そのＩＣカードの利用可能金額だけ利用すると、ＩＣカードをＳＳ協会（ソフトウエアを管理する協会）に届ける。ＩＣカードにはユーザが利用したソフトウエアの利用明細が格納されており、ＳＳ協会はこの利用明細をもとにソフトウエアの著作者に利用料金を支払う。これにより、ソフトウェアのオフラインでの使用を認めながらも、利用頻度に応じた課金が可能となる。
【０００８】
【発明が解決しようとする課題】しかし、利用明細を格納したＩＣカードをＳＳ協会に送付する方法では、ＩＣカードの利用可能金額がなくなる度に、ＳＳ協会から再配布されるのを待つか、代理店で新しいＩＣカードを購入しなければならないという問題点がある。しかも、一般的に履歴データは長大なものになる傾向があるため、ＩＣカードのような記憶容量の少ない媒体に保管すると、頻繁にＩＣカードを交換する必要性が出てくる。
【０００９】そのため、ＩＣカードが生成する課金情報のように確実にセンタに送られるべきデータを、端末装置等に安全に保管できるような技術が必要とされている。すなわち、端末装置に課金情報を保管しておくことができれば、ＩＣカードの記憶容量が少なくても、頻繁にＩＣカードの再発行などをする必要がなく、しかも、オフラインでサービスを利用することができる。さらに、課金情報などの履歴データは数回または数十回に渡って出力されると考えられるため、履歴データの順番の整合性（連鎖）が保たれている必要がある。そして、センタでは、連鎖が崩されていないことを含めて検証できなければならない。なぜなら、途中の履歴データが抜けていることを検出できないと、その部分の利用料金を回収できなくなるからである。

【００１０】本発明はこのような点に鑑みなされたものであり、不正操作を受けること無く端末装置に保管可能であり、且つ順番の整合性が保証されたデータを生成できる被検証データ生成装置を提供することを目的とする。

【００１１】また、本発明の他の目的は、不正操作を受けること無く端末装置に保管可能な形式のデータの連鎖性を含めて検証できるデータ検証装置を提供することである。

【００１２】また、本発明の別の目的は、不正操作を受けること無く端末装置に保管可能であり、且つ順番の整合性が保証されたデータをコンピュータに生成させるための被検証データ生成プログラムを記録した媒体を提供することである。

【００１３】

【課題を解決するための手段】本発明では上記課題を解決するために、被検証データを生成する被検証データ生成装置において、検証値を保持する検証値保持手段と、データ本体を生成するデータ生成手段と、前記データ生成手段によりデータ本体が生成される度に、前記検証値保持手段において保持されている検証値と新たに生成されたデータ本体とに基づいて新たな検証値を生成し、生成した検証値で前記検証値保持手段に保持されている検証値を更新する検証値生成手段と、前記データ生成手段で生成されたデータ本体を順次格納するデータ格納手段と、被検証データ出力要求を受け取ると、前記検証値保持手段に格納されている検証値を用いて署名値を生成し、前記データ格納手段に格納されているデータ本体と前記署名値とを含む被検証データを出力する被検証データ出力手段と、を有することを特徴とする被検証データ生成装置が提供される。

【００１４】この被検証データ生成装置によれば、データ生成手段がデータ本体を生成すると、検証値生成手段により、、検証値保持手段において保持されている検証値と新たに生成されたデータ本体とに基づいて新たな検証値が生成され、生成した検証値で検証値保持手段に保持されている検証値が更新される。一方、データ生成手段で生成されたデータ本体は、順次データ格納手段に格納される。そして、被検証データ出力要求を受け取ると、被検証データ生成装置により、検証値保持手段に格納されている検証値を用いて署名値が生成され、データ格納手段に格納されているデータ本体と前記署名値とを含む被検証データが出力される。

【００１５】また、上記課題を解決するために、データの検証を行うデータ検証装置において、検証値を保持する検証値保持手段と、複数のデータ本文に対して署名値が付加された被検証データを受け取ると、前記検証値保持手段に保持されている検証値と前記複数のデータ本文とから照合用検証値を生成する照合用検証値生成手段と、前記署名値から求められる検証値と前記照合用検証値とを照合し、一致した場合にのみ前記被検証データの内容が正しいと認める認証手段と、前記署名値から求められる検証値と前記照合用検証値とが一致した場合には、前記照合用検証値によって前記検証値保持手段に保持されている検証値を更新する検証値更新手段と、を有することを特徴とするデータ検証装置が提供される。

【００１６】このデータ検証装置によれば、複数のデータ本文に対して署名値が付加された被検証データを受け取ると、照合用検証値生成手段により、検証値保持手段に保持されている検証値と複数のデータ本文とから照合用検証値が生成される。そして、認証手段により、署名値から求められる検証値と照合用検証値とが照合され、一致した場合にのみ被検証データの内容が正しいと認められる。一方、署名値から求められる検証値と照合用検証値とが一致した場合には、検証値更新手段により、検証値保持手段に保持されている検証値が、照合用検証値に更新される。

【００１７】また、上記課題を解説するために、被検証データの生成をコンピュータに行わせるための被検証データ生成プログラムを記録した媒体において、検証値を保持する検証値保持手段、データ本体を生成するデータ生成手段、前記データ生成手段によりデータ本体が生成される度に、前記検証値保持手段において保持されている検証値と新たに生成されたデータ本体とに基づいて新たな検証値を生成し、生成した検証値で前記検証値保持手段に保持されている検証値を更新する検証値生成手段、前記データ生成手段で生成されたデータ本体を順次格納するデータ格納手段、被検証データ出力要求を受け取ると、前記検証値保持手段に格納されている検証値を用いて署名値を生成し、前記データ格納手段に格納されているデータ本体と前記署名値とを含む被検証データを出力する被検証データ出力手段、としてコンピュータを機能させるための被検証データ生成プログラムを記録した媒体が提供される。

【００１８】この媒体に記録されたプログラムをコンピュータに実行させれば、検証値を保持する検証値保持手段と、データ本体を生成するデータ生成手段と、前記データ生成手段によりデータ本体が生成される度に、前記検証値保持手段において保持されている検証値と新たに生成されたデータ本体とに基づいて新たな検証値を生成し、生成した検証値で前記検証値保持手段に保持されている検証値を更新する検証値生成手段と、前記データ生成手段で生成されたデータ本体を順次格納するデータ格納手段と、被検証データ出力要求を受け取ると、前記検証値保持手段に格納されている検証値を用いて署名値を生成し、前記データ格納手段に格納されているデータ本体と前記署名値とを含む被検証データを出力する被検証データ出力手段と、の各処理機能を持ったコンピュータシステムが構築される。

【００１９】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。図１は、本発明の原理構成図である。本発明の被検証データ生成装置は、以下のような要素で構成される。

【００２０】検証値保持手段１は、検証値を保持する。データ生成手段２は、所定のタイミングでデータ本体を生成する。例えば、所定のデータ処理要求を受け取った際に、そのデータ処理の履歴をデータ本体として生成する。

【００２１】検証値生成手段３は、データ生成手段２によりデータ本体が生成される度に、検証値保持手段１において保持されている検証値と新たに生成されたデータ本体とに基づいて新たな検証値を生成する。そして、新たな検証値で検証値保持手段１に保持されている検証値を更新する。データ格納手段４は、データ生成手段１で生成されたデータ本体を順次格納する。被検証データ出力手段５は、被検証データ出力要求を受け取ると、検証値保持手段１に格納されている検証値に基づいて認証子を生成し、生成した認証子とデータ格納手段４に格納されているデータ本体とを結合した被検証データを出力する。

【００２２】これにより、データ処理要求が実行されるたびに、新たなデータ本体がデータ格納手段４に格納されるとともに、検証値保持手段１に保持されている検証値の内容が更新される。そして、被検証データ出力要求が出されると、検証値保持手段１内の検証値に基づく署名値で署名された被検証データが出力される。

【００２３】このようにして出力された被検証データは、署名値が付加されているため、端末装置等に蓄えておいてもデータ本体の内容を改ざんすることができない。しかも、順次生成されるデータ本体とそれ以前に生成された検証値を用いて新たな検証値を生成するため、被検証データの連鎖性も保証される。すなわち、被検証データが多数生成された場合であっても、途中の被検証データが抜けた状態では、サーバなどの検証装置においてそのデータは認証されない。この結果、こまめに被検証データを外部に出力し、オフラインの端末装置などに保存しておくことができるようになり、データ格納手段４の記憶容量が少なくてすむ。

【００２４】ところで、本発明の被検証データ生成装置は、ＩＣカード上で実現することができる。この場合、履歴データをＩＣカードに保持して媒体ごと送付するのではなく、ＩＣカードに検証値を保持することで履歴データをＩＣカードから取り出し、取り出した履歴データは一時的に端末装置に保存する。そして、ネットワークを用いて端末装置から履歴管理センタに履歴データを送付する。これにより、履歴データの正当性を保証しつつ、オフラインでの履歴の回収が可能となる。なお、電子署名等の技術を用いて履歴データ等を安全に取り出せるＩＣカードは既に製品化されており、ＩＳＯ(International Organization for Standardization)／ＩＥＣ(International Electrotechnical Commission) －７８１６でもセキュアメッセージング技術として規定されている。

【００２５】そこで、ＩＣカードから履歴データなどの情報を端末装置へ取り出し、端末装置から任意のタイミングでセンタへ課金情報を転送する場合を例にとり、本発明の第１の実施の形態を以下に説明する。

【００２６】図２は、ＩＣカードを用いた履歴管理システムの概略構成を示す図である。ユーザが使用するパーソナルコンピュータ（ＰＣ）１１０は、インターネットなどのネットワーク１２０を介して履歴管理センタ１３０と繋がっている。履歴管理センタ１３０では、ユーザの登録および、ユーザデータやユーザに提供したサービスの履歴等の管理が行われる。そして、履歴管理センタ１３０は、ＰＣ１１０からの要求に応じて、カプセル化されたソフトウェア（以下、単に「カプセル」という）３００を提供する。ここでいうカプセル化とは、例えばＤＥＳ(Data Encryption Standard)等の暗号アルゴリズムを用いて暗号化し、そのままでは使用できないようにすることを指す。なお、カプセル３００は、ＣＤ－ＲＯＭ等の媒体でユーザに提供することもできる。

【００２７】また、ＰＣ１１０には、ＲＳ－２３２Ｃ（アメリカ電子工業会によって規定されたデータ通信用インタフェース）などのインタフェースにより、リーダ／ライタ１４０が接続されている。ユーザは、このリーダ/ ライタ１４０にＩＣカード２００を接続することで、履歴管理センタ１３０から取得したソフトウェアの復号鍵や使用履歴を取得できる。

【００２８】ＩＣカード２００は、ソフトウェアを提供するプロバイダ若しくはプロバイダの依頼を受けた履歴管理センタ１３０からユーザに渡されるものである。なお、この例では、ＰＣ１１０によってサービスを利用するものとしているが、サービスを利用するためのローカルな端末装置はＰＣには限定されず、例えばワークステーションであったり、サーバであったり、ＡＴＭ(Auto Teller Machine) 端末であったりする。

【００２９】図３は、カプセル化されたソフトウエアの構成を示す図である。カプセル３００の内容は、ヘッダ部３１０と、暗号化されたソフトウェア３２０とに分かれている。ヘッダ部３１０には、カプセルを識別するためのカプセルＩＤ３１１、利用料金を算出するための課金情報３１２、及びソフトウェアの復号鍵を生成するための復号鍵生成データ３１３が含まれている。なお、プロバイダにより作成されたソフトウェアは、センタまたはそれに準ずる機関によりカプセル化される。

【００３０】図４は、ＩＣカードのハードウェア構成を示す図である。ＩＣカード２００は、ＣＰＵ２１０を中心として、１つのコンピュータシステムが構築されている。ＣＰＵ２１０には、内部のシステムバスを介して他

の各種要素が接続されている。ＲＡＭ(Random Access Memory)２２０は、ＣＰＵ２１０が処理すべきデータを一時的に格納する。ＲＯＭ(Read Only Memory)２３０は、ＩＣカード２００に必要な機能をＣＰＵ２１０に実行させるためのプログラムが格納されている。入出力装置（Ｉ／Ｏ）２４０は、所定の規格に従って、リーダ／ライタ１４０との間でデータ通信を行う。ＰＲＯＭ(Programmable Read Only Memory) ２５０は、暗号化された復号鍵生成データ３１３から復号鍵を生成するための秘密情報などが格納されている。なお、上記のＰＲＯＭ２５０は、データの書き換えが可能であり、且つ電源の供給が無くてもデータを保持できる記憶装置（不揮発性メモリ）であれば、他の記憶装置であってもよい。

【００３１】このようなハードウェア構成のＩＣカード２００によって、以下のような処理機能が実現されている。図５は、ＩＣカードの処理機能を示すブロック図である。

【００３２】ログ生成部２０１は、ＰＣ１１０からヘッダ部を受け取ると、ログを生成する。ただし、ログ数カウンタ２０４ａの値が格納可能ログ数２０１ａの値と等しい場合には、ログを生成せずにＰＣ１１０に対してエラーを返す。格納可能ログ数２０１ａは、ログセット格納部２０４に格納できるログの数が予め設定されており、その値はＩＣカード２００のＰＲＯＭ２５０の容量によって定まる。

【００３３】検証値格納部２０２には、ログの連鎖が正しいことをＩＣカード１１０と履歴管理センタ１３０とで検証するための検証値が格納されている。検証方法については後述する。

【００３４】ＭＤ５演算部２０３は、ログ生成部２０１で新たなログが生成される度に、新たな検証値を生成する。具体的には、まず、ログ生成部２０１で生成されたログと検証値格納部２０２に格納されている検証値とを結合する。さらに、結合された値に対して一方向性ハッシュ関数「ＭＤ５」(R.Rivest:The MD5 Message-Digest Algorithm, Internet RFC 1321(1992))を用いてメッセージ・ダイジェストを計算し、検証値を生成する。そして、生成された検証値を用いて、検証値格納部２０２内の検証値の値を更新する。

【００３５】なお、上記の例では一方向性ハッシュ関数「ＭＤ５」を用いて検証値を生成しているが、ここでいう一方向性とは計算結果から計算される前の値を逆算することができないことを指し、このような性質を持つか、あるいは持つと思われている関数であれば「ＭＤ５」と代替可能である。

【００３６】ログセット格納部２０４は、複数のログの組であるログセットを格納しており、ログ生成部２０１が生成したログを逐次ログセットに連結する。ログ数カウンタ２０４ａは、ログセット格納部２０４に格納されたログ数をカウントしている。このカウンタの値は、ログセット格納部２０４内のログセットが消去された際に「０」にリセットされる。

【００３７】復号鍵生成部２０５は、ログ生成部２０１でログが生成されると、ＩＣカード２００内の秘密データとカプセル３００の復号鍵生成データ３１３とにより復号鍵を生成し、復号鍵をＰＣ１１０に転送する。

【００３８】ログ管理部２０６は、ＰＣ１１０からログセット出力要求を受け取ると、ログセット格納部２０４に格納されているログセットをＰＣ１１０に対して出力する。なお、出力するログセットには、ログセットシリアル番号カウンタ２０６ａの値を付加する。ログセットシリアル番号カウンタ２０６ａは、ログセットの通し番号を格納しており、ログセットが消去される度に、値を１だけインクリメントする。また、ログセットの出力が可能であるか否かは、ログ出力状態２０６ｂによって管理している。ログ出力状態２０６ｂには、「ＦＡＬＳＥ」と「ＴＲＵＥ」とがある。「ＦＡＬＳＥ」の場合には、ログセットを出力することができず、「ＴＲＵＥ」の場合には、ログセットの出力が可能である。

【００３９】稼動制御部２０７は、ログ生成部２０１の機能を含めＩＣカード２００の基本的な機能の起動と停止とを管理している。具体的には、利用期限２０７ａの範囲を超えている場合、あるいは生成可能ログ数減算カウンタ２０７ｂの値が０である場合には、ＩＣカード２００の機能を停止する。そして、利用延長データ認証部２０８からの指令によって、停止していた機能を起動する。なお、利用期限２０７ａは、ＩＣカード２００の利用期限が設定されている。生成可能ログ数減算カウンタ２０７ｂは、ログセットを履歴管理センタ１３０に送付せずにカプセルを利用可能な限度回数が初期値として設定されており、ログ生成部２０１によってログが生成される度に値が１だけ減算される。

【００４０】利用延長データ認証部２０８は、ＰＣ１１０から利用延長データを受け取ると、利用延長データの認証を行う。そして、認証に成功した場合には、利用延長データを用いて、利用期限２０７ａと生成可能ログ数減算カウンタ２０７ｂとを更新する。

【００４１】以上のような機能を有するＩＣカード２００を用いて、カプセル３００内の暗号化されたソフトウェア３２０を実行するには、次のような作業を行う。まず、ユーザは、ＩＣカード２００をリーダ／ライタ１４０に接続する。そして、ＰＣ１１０によってカプセル３００に起動をかける。

【００４２】図６は、カプセル実行開始手順を示すフローチャートである。この図において、点線の左側に示す処理はＰＣ１１０で行われる処理であり、点線の右側に示す処理はＩＣカードで行われる処理である。

［Ｓ１］ＰＣ１１０が、カプセル３００内のヘッダ部３１０をＩＣカード２００へ転送する。

［Ｓ２］ヘッダ部３１０を受け取ったＩＣカード２００

では、まず、ログ生成部２０１が新たなログを生成し、そのログをＭＤ５演算部２０３とログセット格納部２０４に渡す。

［Ｓ３］ＭＤ５演算部２０３が、受け取ったログと検証値格納部２０２に格納されている検証値とから新たな検証値を生成し、検証値格納部２０２内の検証値を更新する。

［Ｓ４］ログセット格納部２０４が、格納しているログセットに、受け取ったログを連結する。なお、この時、ログ出力状態２０６ｂが「ＴＲＵＥ」の場合には、ログ管理部２０６がログ出力状態２０６ｂを「ＦＡＬＳＥ」にする。

［Ｓ５］ログ数カウンタ２０４ａが、保持している値を１だけカウントアップする。また、生成可能ログ数減算カウンタ２０７ｂが、保持している値を１だけカウントダウンする。

［Ｓ６］復号鍵生成部２０５が復号鍵生成データ３１３と秘密データとを用いて復号鍵を生成し、ＰＣ１１０へ転送する。

［Ｓ７］復号鍵を受け取ったＰＣ１１０が、その復号鍵で暗号化されたソフトウェア３２０を復号し、実行する。

【００４３】このようにして、ユーザがカプセル内のソフトウェアを実行する度に、その利用履歴がログとしてＩＣカード２００内で保持される。図７は、ログの構成例を示す図である。ログ４００には、カプセルＩＤ４０１、ログ作成時刻４０２、及び課金情報４０３が含まれている。ところで、ログ４００は一時的にＩＣカード２００内に格納されるので、各要素はできるだけ少ないバイト数で構成することが望ましい。たとえばシステム時刻をＵＴＣ(Coordinated Universal Time:世界協定時刻）に対応する４バイトで表現しているとすると、ログ作成時刻にはＵＴＣ４バイトをすべて入れる必要はなく、たとえば細かい値が必要無いならば全４バイトのうちの上位３バイトを入れればよく、また相対値のみがわかればよいなら下位３バイトを入れればよい。

【００４４】次に、ＩＣカード２００の内部で保持されているログセットを履歴管理センタ１３０で回収し、その値を検証する方法について説明する。ログセット格納部２０４内の複数のログは、生成された順番に結合され、ログセットとしてＩＣカード２００内の不揮発性メモリ（ＰＲＯＭ２５０）に格納されるが、ＩＣカード２００の記憶容量の関係から大量のログデータをＩＣカード２００内に記憶することは不可能であり、ＩＣカード２００には予め格納可能ログ数２０１ａが設定されている。そして、ログ数カウンタ２０４ａの値がこの格納可能ログ数２０１ａに達すると、ログ生成部２０１が新たなログを生成できず、復号鍵生成部２０５も復号鍵を出力しない。したがって、このままではソフトウェアの実行ができない。

【００４５】この状態になるとユーザはＰＣ１１０を操作し、ＰＣ１１０からＩＣカード２００に対しログ出力要求を出す。ログ出力要求を受け取ったＩＣカード２００は、ログセットにＩＣカード２００の署名を施した署名付きログセットを出力する。ちなみにユーザはログ数が一杯になる前にもログ出力を行うことが可能である。

【００４６】図８は、署名付きログセットの構成を示す図である。署名付きログセット５００は、ユーザＩＤ５０１、ログセット作成時刻５０２、ログセットシリアル番号５０３、署名値５０４、ログ数５１１およびｎ個のログ５１２とから構成される。

【００４７】図９は、ログセットの署名値５０４として署名される平文の構成例を示す図である。ここではＩＣカード２００の署名鍵（秘密鍵）で署名される平文７００を暗号化する場合について説明する。署名に用いる暗号化方式は公開鍵暗号方式に限らず履歴管理センタ１３０とＩＣカード２００で秘密鍵を安全な方法で共有できれば慣用鍵暗号方式を用いてもよい。

【００４８】署名される平文７００は、ユーザＩＤ７０１、ログセット作成時刻７０２、ログセットシリアル番号７０３、ログ数７０４および検証値７０５で構成される。検証値７０５はログセット５００を出力するときにＩＣカード２００の検証値格納部２０２に保持されている検証値と同一のものである。すなわち、これらの情報からなる平文７００をＩＣカード２００の秘密鍵で暗号化することで、署名値５０４が得られる。

【００４９】図１０は、ＩＣカードからログセットを出力する手順を示すフローチャートである。この図において、点線の左側に示す処理はＰＣ１１０で行われる処理であり、点線の右側に示す処理はＩＣカードで行われる処理である。

［Ｓ１１］ＰＣ１１０が、ＩＣカード２００に対してログセット出力要求を出す。

［Ｓ１２］ＩＣカード２００では、ログ管理部２０６が、ログセット出力要求を受け取り、ログ出力状態２０６ｂを「ＴＲＵＥ」にし図８に示したような署名付きログセット５００を出力する。

［Ｓ１３］ＰＣ１１０が、ＩＣカード２００からログセットを取得する。

［Ｓ１４］ＰＣ１１０は、ログセットを正常に取得できたか否かを判断する。ログセットをＰＣ１１０が正常に取得できていればステップＳ１５に進む。一方、ログセットが正常に取得できなかった場合は、ステップＳ１１に進み、再度ＩＣカード２００に対してログセット出力要求を出し、ステップＳ１１～Ｓ１３を繰り返す。

［Ｓ１５］ＰＣ１１０が、ＩＣカード２００に対してログセット消去要求を出す。

［Ｓ１６］ＩＣカード２００では、ログ管理部２０６がログセット消去要求を受け取り、ログ出力状態２０６ｂが「ＴＲＵＥ」であるか否かを判断する。「ＴＲＵＥ」

であればステップＳ１７に進み、「ＴＲＵＥ」でなければステップＳ２１に進む。

［Ｓ１７］ログ管理部２０６が、ログセット格納部２０４内のログセットを消去する。

［Ｓ１８］ログ数カウンタ２０４ａが、保持している値を「０」にリセットする。

［Ｓ１９］ログセットシリアル番号カウンタ２０６ａが、保持しているログセットシリアル番号を１だけインクリメントする。

［Ｓ２０］ログ管理部２０６は、正常終了を表すステータスをＰＣ１１０に返し、処理を終了する。

［Ｓ２１］ログ出力状態２０６ｂが「ＦＡＬＳＥ」ならばログセットの消去は行わずエラーステータスをＰＣ１１０に返す。

【００５０】なお、ログセット出力中にエラーが発生した場合のことを考慮して、ＩＣカード２００をリセット状態にした場合はログ出力状態２０６ｂは「ＦＡＬＳＥ」となる。

【００５１】以上がログセットを出力する手順であるが、このようにログセットの出力とログセットの消去を別々の命令で行うのは、以下のようなＩＣカード２００のプロトコル形式に依存した理由による。ＩＣカード２００のデータ転送プロトコルＴ＝０およびＴ＝１（ＩＳＯ／ＩＥＣ７８１６－３）では、ＩＣカード２００からＩＦＤ(Interface Device）（ここではＰＣ１１０を示す）にデータを出力した後、ＩＣカード２００は受信待ち状態となりＩＣカード内で処理を行うことができない。もし、１つのコマンドでログセットの出力と消去を行おうとすると、ログセットを消去した後でログセットを出力しなければならなくなるので、ログセットの出力が通信の過程で失敗した場合にログセットが失われてしまうことになる。

【００５２】一方、単純にログセット出力コマンドとログセット消去コマンドの２つに分けただけだと、ユーザが誤ってログセットを出力する前にログセット消去コマンドをＩＣカードに発行してしまうと、ログセットが失われてしまう。したがって本発明ではＩＣカードにログ出力状態２０６ｂを持たせ、ログセット２０３が出力された場合のみログ出力状態２０６ｂが「ＴＲＵＥ」となりログセットが消去可能となることで、上記の問題を解決している。ログセット消去後、ソフトウェアの起動を行うと、ログがＩＣカード内で生成され、ログ出力状態２０６ｂが「ＦＡＬＳＥ」状態となるので、再びログセット出力を行わない限りログセットを消去できない。

【００５３】ＩＣカード２００から出力されたログセット５００は、一旦ＰＣ１１０で保管される。ＰＣ１１０で保管されたログセット５００はある一定期間ごとに履歴管理センタ１３０で回収して、そのログの内容を基にユーザから料金を徴収しソフトウェアの著作者に料金を分配する。履歴管理センタ１３０で効率よく履歴を回収するために、ＩＣカード２００には利用期限２０７ａと生成可能ログ数という２つの値があらかじめ設定されている。利用期限２０７ａとはＩＣカード２００を利用可能な期日を表し、利用期限２０７ａを過ぎた後はＩＣカード２００が停止状態となり、カプセルを利用できなくなる。再び利用可能とするためには履歴管理センタ１３０にこれまで出力したログセットを送信し利用延長データを取得する必要がある。また、生成可能ログ数は、生成可能ログ数減算カウンタ２０７ｂの初期値として設定され、生成可能ログ数減算カウンタ２０７ｂの値が０になるとＩＣカード２００が停止状態となり、カプセル３００を利用できなくなる。再び利用可能とするためには、履歴管理センタ１３０にログセットを送信し利用延長データを取得する必要がある。

【００５４】ところで、ユーザごとのログセットの検証を履歴管理センタで行うには、履歴管理センタ１３０において、以下のようなユーザデータベース（ＤＢ）を有している必要がある。

【００５５】図１１は、履歴管理センタで管理しているユーザＤＢの例を示す図である。ユーザＤＢ９００には、各ユーザの履歴管理用データ９１０がある。この履歴管理用データ９１０には、ユーザＩＤ９１１、前回検証したログセットの最終シリアル番号９１２、最終シリアル番号に対応するログセットの検証値９１３、及びその他認証等に用いるユーザ固有のデータ９１４が含まれている。

【００５６】ユーザは上記の利用限度が来てカプセルが利用できなくなったか、またはそれ以前の任意のタイミングで、ＩＣカード２００から出力したログセットをまとめて履歴管理センタ１３０に送付する。このときユーザはＩＣカード２００から出力したログセットをログセットシリアル番号順に送信することが望ましいが、履歴管理センタ１３０でログセットシリアル番号をソーティングできればその必要はない。但し、出力したログセットが全て揃っている必要がある。図１２は、履歴管理センタにおけるログセットの検証手順を示すフローチャートである。この処理は全て、履歴管理センタ１３０のコンピュータで行われる。

［Ｓ３１］ログセットを受け取る。

［Ｓ３２］受け取った複数のログセットをシリアル番号順にソートすると共に、ユーザＩＤを基にユーザＤＢ９００から対応するユーザの履歴管理用データ９１０を取得し、今回受け取ったシリアル番号の最小値が履歴管理センタ１３０で保管している、ユーザの前回の最終ログセットシリアル番号９１２と連鎖していることを確認する。次に、今回受け取った複数のログセットのシリアル番号の連鎖を確認しログセットに抜けが無いことを確認したらステップＳ３３に進む。ログセットに抜けがあった場合はステップＳ３５に進む。

［Ｓ３３］ログセットの署名に格納されている検証値７

０５を用いてログの連鎖の検証を行う。検証が正しく行われればステップＳ３４に進み、検証値が正しく行われなければステップＳ３５に進む。なお、検証手順の詳細は後述する。

［Ｓ３４］利用延長データを発行し、ＰＣ１１０へ転送する。

［Ｓ３５］ＰＣ１１０にエラーステータスを返す。

【００５７】これにより、ユーザは利用延長データを取得することが出来る。図１３は、検証値の検証手順の詳細を示す図である。この処理は、全て履歴管理センタ１３０のコンピュータで行われる。

［Ｓ３３１］ログセットの検証を行う。検証には、ログセット５００中の複数のログ５１２ａ～５１２ｎ等を用いる。ここで、ログセットが複数ある場合には、シリアル番号順に検証が行われる。

【００５８】まず、ログセットの出所が正しいことを検証する。これは、ログセット５００内の署名値５０４をユーザＩＤ５０１に対応したＩＣカード２００の公開鍵により検証し、ログセット５００の値と署名値の平文７００中のデータとの整合を確認する。

【００５９】次に最初のログ５１２ａと前回の検証値９１３とを連結し、ＩＣカード２００が検証値を生成するのと同じ方法で、検証値を生成する。すなわち、結合された値に対して一方向性ハッシュ関数ＭＤ５を用いてメッセージ・ダイジェストを計算し、検証値９１３ａを生成する。

【００６０】次にログ５１２ｂと検証値９１３ａとを連結し、検証値９１３ｂを生成する。以下ログ５１２ｃ～ログ９１３ｎまで、同様の演算を繰り返し、ログ５１２ｎと検証値９１３ｍの結合値に対するメッセージ・ダイジェストである検証値９１３ｎを生成する。

［Ｓ３３２］検証値７０５と検証値９１３ｎとを比較し、値が一致する場合にはステップＳ３３３に進む。検証値７０５と検証値９１３ｎとが一致しない場合はステップＳ３３４に進む。

［Ｓ３３３］次のログセットが存在する場合は上記と同様の手順で検証値を検証し、次のログセットが存在しない場合、すなわちユーザから受け取ったログセットの検証が全て終了した場合は、履歴管理センタで管理しているユーザの履歴管理データ９１０中の前回の最終シリアル番号９１２を今回検証した最後のログセットのシリアル番号で更新し、前回の最終検証値９１３を今回検証した最後のログセットの検証値で更新する。

［Ｓ３３４］エラーステータスをユーザに返し、処理を終了する。

【００６１】このようにして、履歴管理センタ１３０がログセットを検証し、利用延長データを発行する。図１４は、利用延長データの構成例を示す図である。この図は、利用延長データの署名前の平文８００を示している。この平文８００には、生成可能ログ数８０１、有効期限８０２、検証値８０３を含んでいる。ここでの検証値８０３には最後に検証したログセットの検証値が入る。履歴管理センタ１３０ではこの平文８００に対して履歴管理センタ１３０の秘密鍵で署名し、利用延長データとしてユーザに送信する。

【００６２】ユーザは、受け取った利用延長データをＩＣカード２００に入力する。ＩＣカード２００では、利用延長データ認証部２０８が利用延長データの署名を予め登録されている履歴管理センタ１３０の公開鍵で検証する。さらに、利用延長データ中の検証値８０３と検証値格納部２０２内の検証値が一致したら、ＩＣカード２００の利用期限２０７ａを利用延長データ中の有効期限８０２で更新し、生成可能ログ数減算カウンタ２０７ｂを利用延長データ中の生成可能ログ数８０１で更新する。また、ＩＣカード２００が停止状態の場合は、稼動制御部２０７が停止状態を解除する。

【００６３】このように、本発明によれば利用履歴等の長大なデータをブロック化して、ユーザの任意のタイミングにおいてネットワークで安全に送付可能である。また、ブロック化されたデータごとに認証が可能であり、かつブロックの連鎖も認証することができる。また、本発明によればログデータがＩＣカード等の履歴格納媒体の記憶容量を越える場合でも、一旦履歴格納媒体から履歴データを出力して、新たに格納することが可能なので、履歴データの管理を履歴格納媒体の記憶容量に何ら制限されずに行うことができる。

【００６４】なお、以上の説明ではログセットが回収可能な場合の例を説明したが、何らかの事後によりログセットの一部が破壊された場合でも、本発明ではログセットをログシリアル番号で管理し、またログセットごとにＩＣカードの署名を施しているので、破壊されたログセット以外の検証を行うことが可能である。

【００６５】次に、第２の実施の形態について説明する。この実施の形態は、ログセットを出力してから利用延長データを受け取るまでの間にも、カプセル３００を利用できるようにしたものである。すなわち、第１の実施の形態では、ログセット５００を履歴管理センタ１３０に送付し利用延長データを受け取るまでに、カプセルを実行してしまうと、ＩＣカード２００内でログが新たに生成され検証値が更新されてしまう。すると、利用延長データを検証できない。この問題を防ぐために、ユーザが履歴管理センタ１３０にログセットを送付後、利用延長データを受け取るまでカプセルを利用できないようにすることが考えられるが、ネットワークを利用するとしても、ある程度の時間ユーザはカプセル３００を使用できなくなり不便である。そこで第２の実施の形態では、ユーザが履歴管理センタ１３０にログセットを送付後でも、ＩＣカード内にログを保管できる範囲内であればカプセルを利用可能としている。

【００６６】なお、本実施の形態は、第１の実施の形態

と比べ利用延長データ認証部２０８の処理機能が異なるだけであるため、第１の実施の形態の各要素に付加した符号を用いて本実施の形態を説明する。

【００６７】図１５は、第２の実施の形態における利用延長データの認証処理を示す図である。ここでは、ユーザが履歴管理センタ１３０に対しこれまでに出力したログセットを送付した後、カプセルをｎ回利用した場合を想定する。図に示すように、ログセット格納部２０４にはｎ個のログ２０４ａ～２０４ｎが格納されている。この状態で、ユーザが履歴管理センタ１３０から利用延長データ８００を受け取り、ＩＣカード２００へ入力すると、以下の処理が行われる。

［Ｓ４１］ＩＣカード２００では、利用延長データ認証部２０８が、利用延長データの署名を履歴管理センタ１３０の公開鍵で検証し利用延長データ中の検証値８０３を取得する。つぎに、ログセット格納部２０４内の最初のログ２０４ａと利用延長データ中の検証値８０３を連結して、ＭＤ５演算部２０３が検証値を生成するときと同じ方法で検証値８０３ａを生成する。以下同様にログ２０４ｂ～２０４ｎと生成された検証値８０３ａ～８０３ｍにより、順次検証値が生成され最後に検証値８０３ｎが生成される。

［Ｓ４２］利用延長データ認証部２０８が、検証値格納部２０２内の検証値２０２ａと検証値８０３ｎとを比較し、それぞれの値が一致した場合はステップＳ４３に進み、一致しなかった場合はステップＳ４４に進む。

［Ｓ４３］利用延長データ認証部２０８が、ＩＣカード２００の利用期限２０７ａを利用延長データ中の有効期限８０２で更新し、生成可能ログ数減算カウンタ２０７ｂを利用延長データ中の生成可能ログ数８０１からログ数カウンタ２０４ａの値（＝ｎ）を減算した値で更新する。さらに、ＩＣカード２００が停止状態の場合は、稼動制御部２０７が停止状態の解除を行う。

［Ｓ４４］検証値２０２ａと検証値８０３ｎとが一致しなかった場合は、利用延長データ認証部２０８が処理を中断しエラーを返す。

【００６８】このようにして、ログセットを出力してから利用延長データを受け取るまでの間においても、カプセルを使用することが可能となる。なお、以上の例ではＩＣカード内で、ログセットに格納されたログの検証値を検証することで利用延長データ中の検証値を検証したが、別の方法としては、検証値格納部２０２に格納される検証値とは別に、第２の検証値として前回出力されたログセットの検証値を保管しておき、利用期限データ中の検証値と第２の検証値とを比較して利用延長データ中の検証値を検証を行うことも考えられる。

【００６９】なお、上記のＩＣカードの有する機能の処理内容は、ＲＯＭに格納されたプログラムをＩＣカード内のＣＰＵが実行することで実現されているが、このプログラムを他のコンピュータで読み取り可能な記録媒体に格納しておくこともできる。コンピュータで読み取り可能な記録媒体としては、磁気記録装置や半導体メモリ等がある。市場を流通させる場合には、ＣＤ－ＲＯＭやフロッピーディスケット等の可搬型記録媒体にプログラムを格納して流通させたり、ネットワークを介して接続されたコンピュータの記憶装置に格納しておき、ネットワークを通じて他のコンピュータに転送することもできる。コンピュータで実行する際には、コンピュータ内のハードディスク装置等にプログラムを格納しておき、メインメモリにロードして実行する。

【００７０】

【発明の効果】以上説明したように本発明の被検証データ生成装置では、データ生成手段がデータ本文を生成する度に、そのデータ本文を用いて検証値を生成し、その検証値を用いて被検証データの署名値を生成するようにしたため、署名付きの被検証データを端末装置などに保管しておき、ユーザの任意のタイミングにおいてネットワークで安全にセンタに送付できる。また、被検証データごとに認証が可能であり、かつ被検証データの連鎖も認証することができるため、データ格納手段に長大なデータを保存する必要がなくなり、データ格納手段の記憶容量が少なくてすむ。

【００７１】また、本発明のデータ検証装置では、データの検証を行う度に、最後に得られた検証値を保持しておき、保持している検証値を用いて次の被検証データの検証を行うようにしたため、被検証データの連鎖を認証することができる。

【００７２】また、本発明の被検証データ生成プログラムを記録した媒体では、記録されているプログラムをコンピュータに実行させれば、データ生成手段がデータ本文を生成する度にそのデータ本文を用いた検証値を生成し、その検証値を用いて署名値を生成するような機能をコンピュータに持たせることができるため、端末装置などに一時的に保管しても不正を働くことが出来ないような連鎖性を保証した被検証データをコンピュータに生成させることが可能となる。

【図面の簡単な説明】

【図１】本発明の原理構成図である。

【図２】ＩＣカードを用いた履歴管理システムの概略構成を示す図である。

【図３】カプセル化されたソフトウエアの構成を示す図である。

【図４】ＩＣカードのハードウェア構成を示す図である。

【図５】ＩＣカードの処理機能を示すブロック図である。

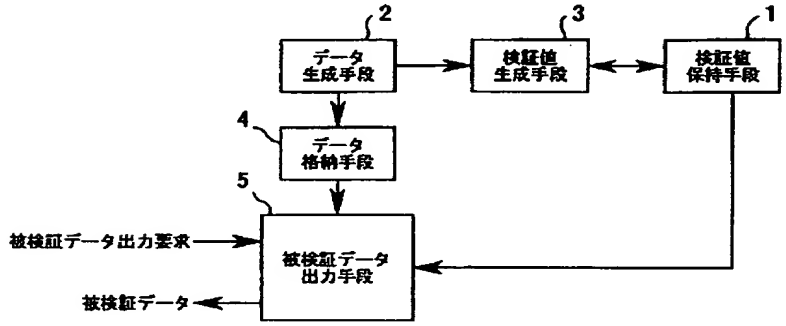
【図６】カプセル実行開始手順を示すフローチャートである。

【図７】ログの構成例を示す図である。

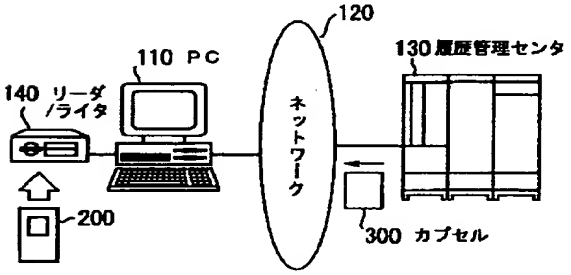
【図８】署名付きログセットの構成を示す図である。

【図９】ログセットの署名値として署名される平文の構成例を示す図である。
【図１０】ＩＣカードからログセットを出力する手順を示すフローチャートである。
【図１１】履歴管理センタで管理しているユーザＤＢの例を示す図である。
【図１２】履歴管理センタにおけるログセットの検証手順を示すフローチャートである。
【図１３】検証値の検証手順の詳細を示す図である。
【図１４】利用延長データの構成例を示す図である。
【図１５】第２の実施の形態における利用延長データの認証処理を示す図である。
【符号の説明】
1　検証値保持手段
2　データ生成手段
3　検証値生成手段
4　データ格納手段
5　被検証データ出力手段

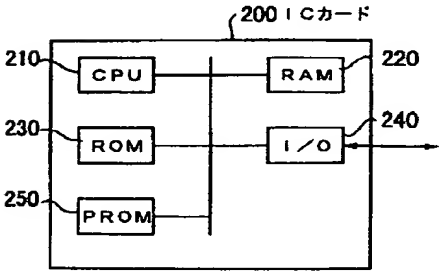
【図１】



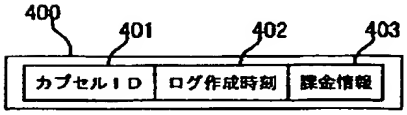
【図２】



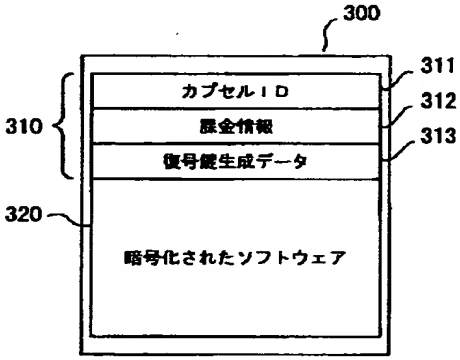
【図４】



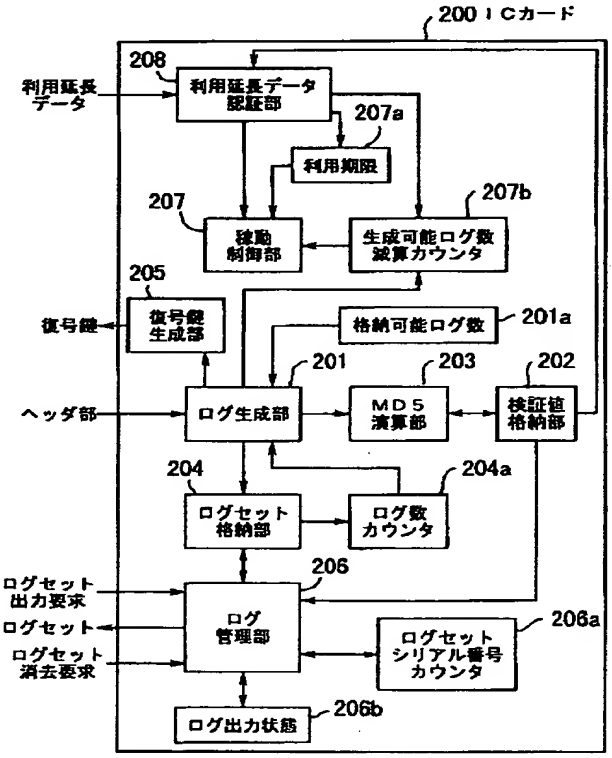
【図７】



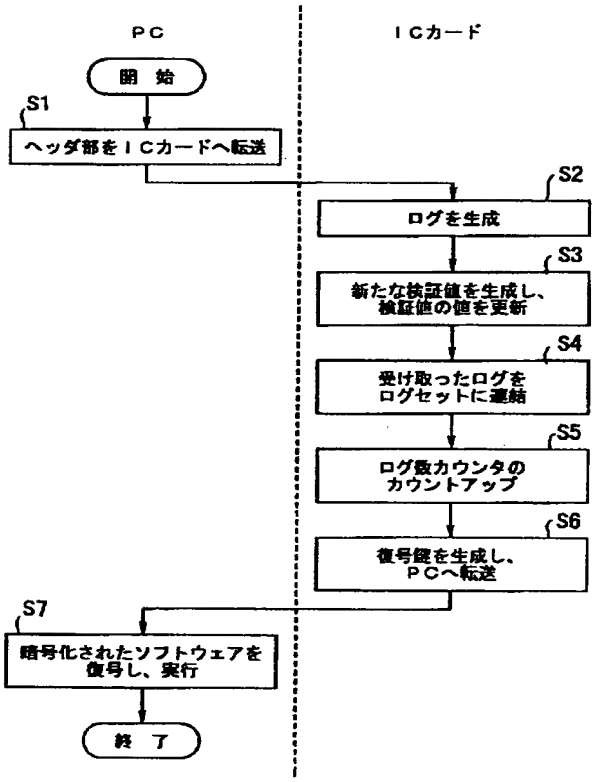
【図３】



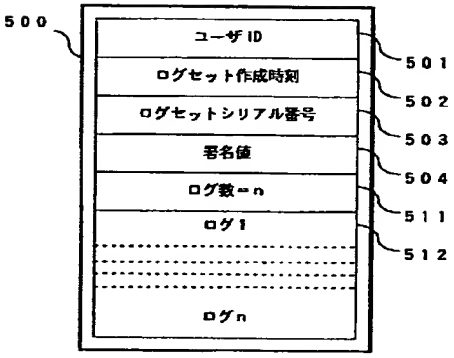
【図５】



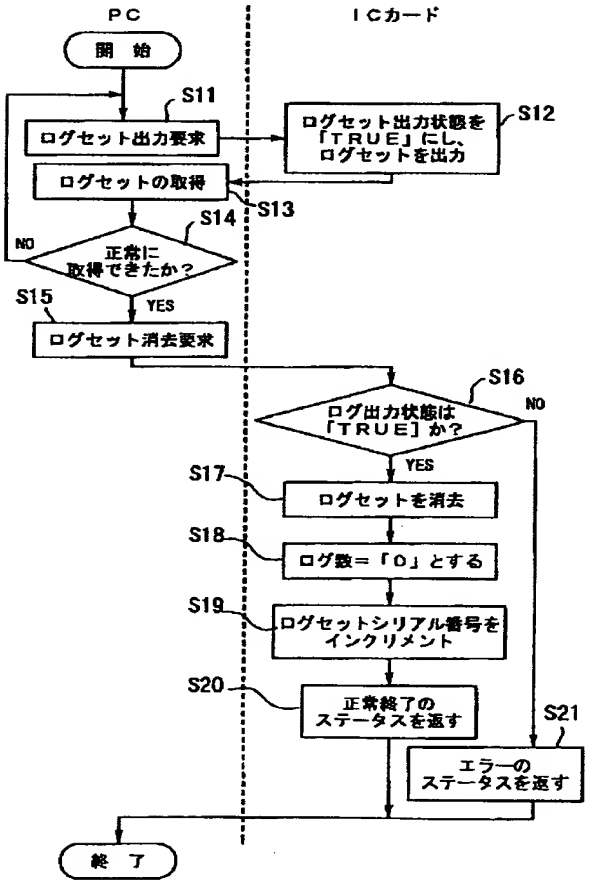
【図６】



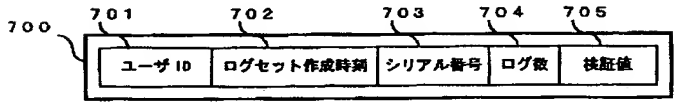
【図８】



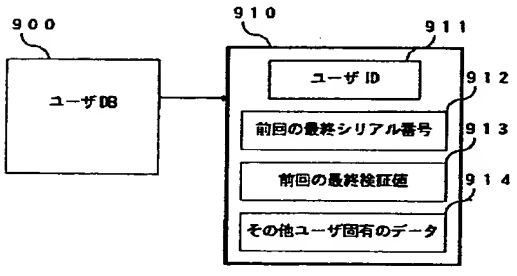
【図１０】



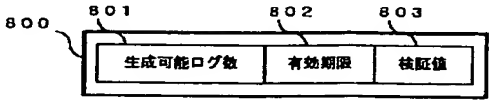
【図９】



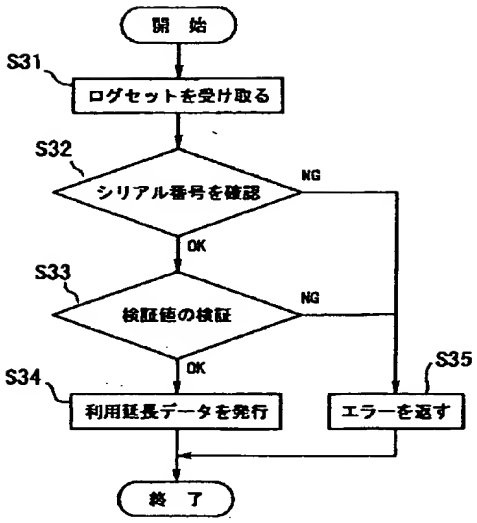
【図１１】



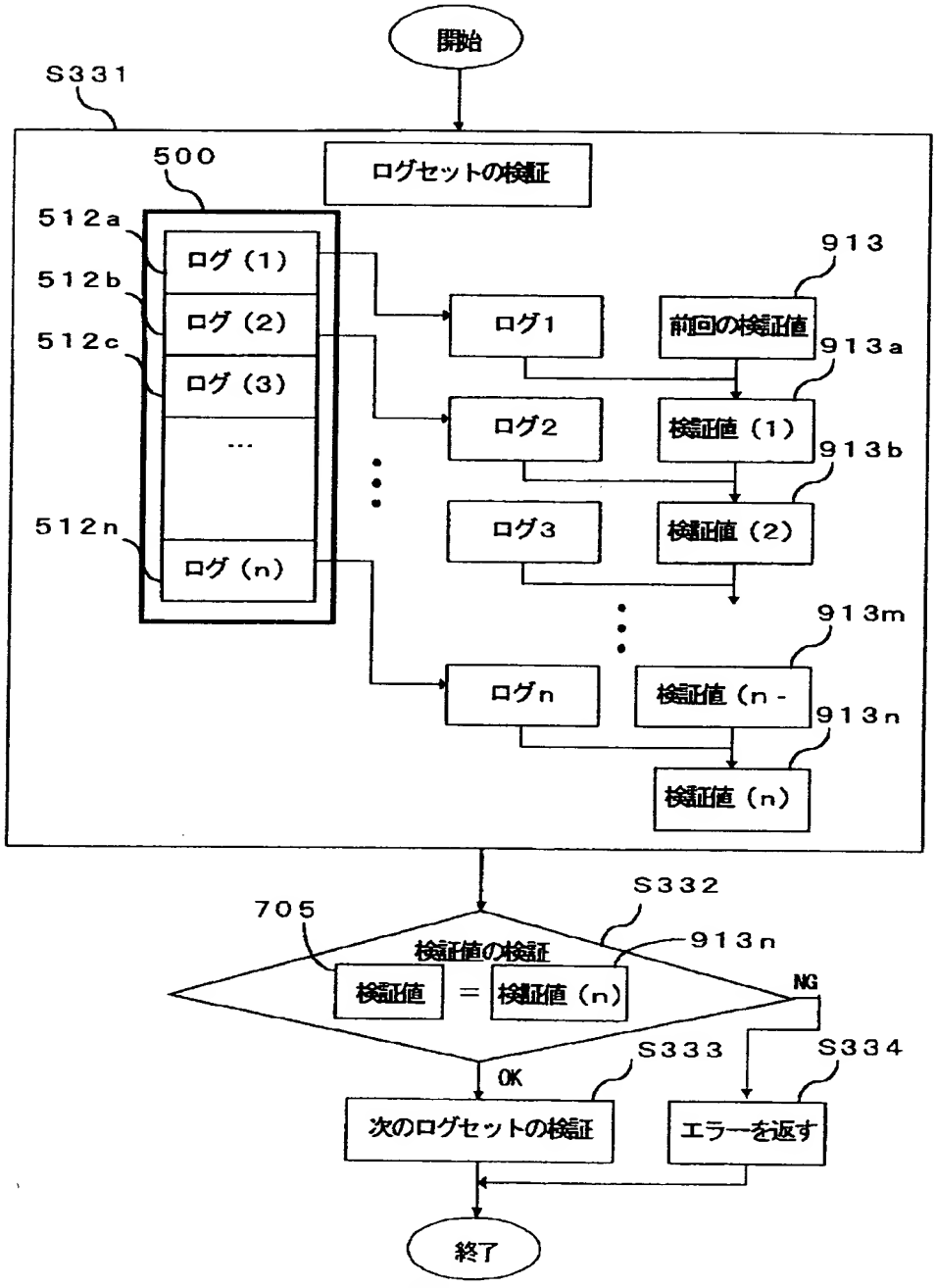
【図１４】



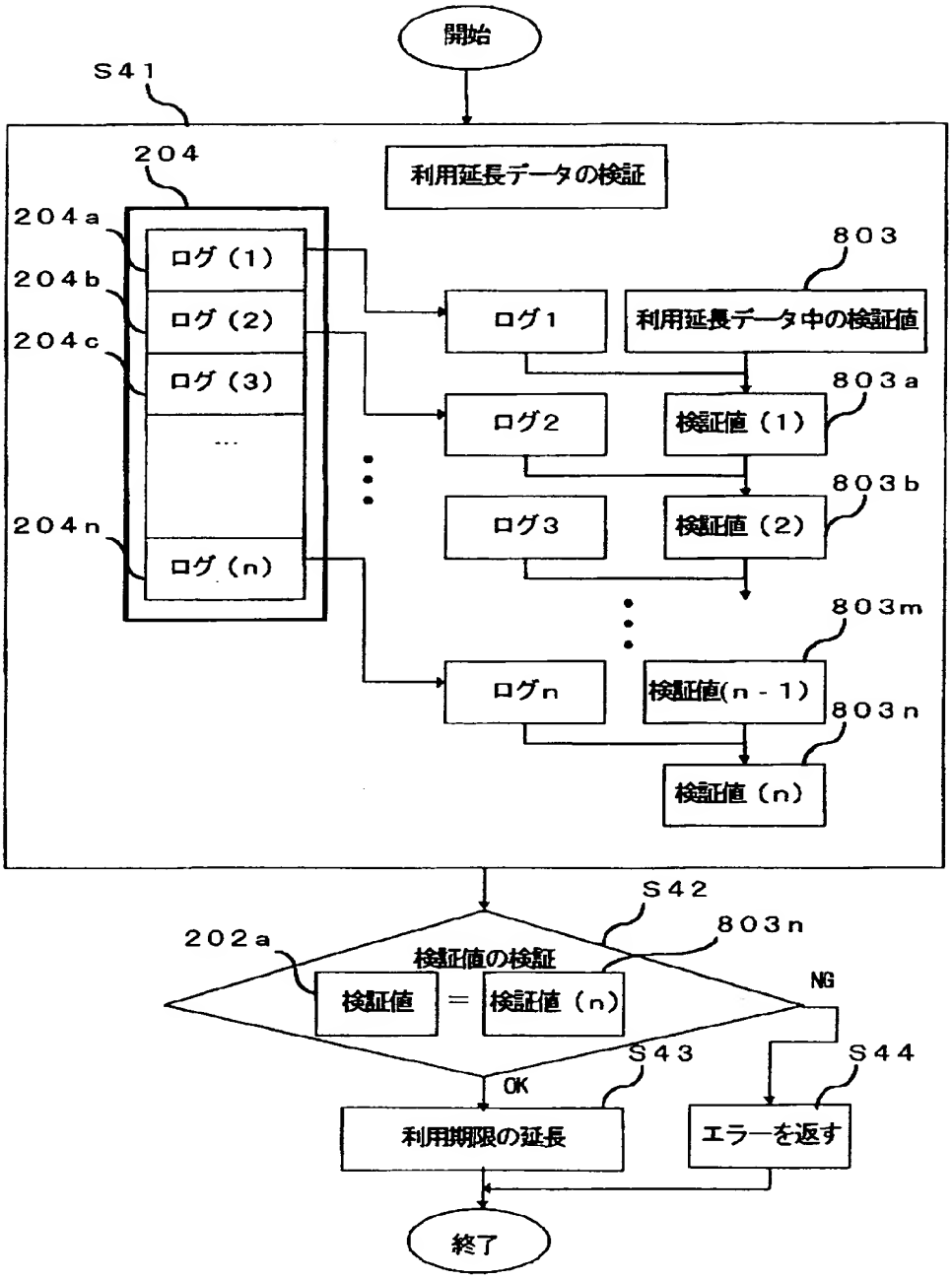
【図１２】


開　始
S31
ログセットを受け取る
S32
シリアル番号を確認
NG
OK
S33
検証値の検証
NG
OK
S34
利用延長データを発行
S35
エラーを返す
終　了

【図１３】


開始
S331
500
ログセットの検証
512a
512b
512c
512n
ログ（1）
ログ（2）
ログ（3）
…
ログ（n）
913
前回の検証値
913a
913b
913m
913n
ログ1
ログ2
ログ3
ログn
検証値（1）
検証値（2）
検証値（n-
検証値（n）
S332
705
検証値の検証
検証値
＝
検証値（n）
NG
OK
S333
S334
次のログセットの検証
エラーを返す
終了

【図１５】


開始
S41
204
利用延長データの検証
204a
204b
204c
204n
ログ（1）
ログ（2）
ログ（3）
...
ログ（n）
803
利用延長データ中の検証値
ログ1
ログ2
ログ3
ログn
803a
検証値（1）
803b
検証値（2）
803m
検証値(n－1)
803n
検証値（n）
S42
202a
検証値の検証
検証値
＝
検証値（n）
NG
OK
S43
S44
利用期限の延長
エラーを返す
終了